BWB:RCH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
– X

IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:	AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT
THE PREMISES KNOWN AND DESCRIBED AS A BLACK IPHONE CELLULAR TELEPHONE, MODEL A1387 (EMC 2430), SEIZED ON OR ABOUT DECEMBER 20, 2014	(T. 18, U.S.C., § 1546(a))

– X

EASTERN DISTRICT OF NEW YORK, SS:

MICHAEL FLAHERTY, being duly sworn, deposes and states that he is a Special Agent with the Diplomatic Security Service ("DSS"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in the PREMISES KNOWN AND DESCRIBED AS A BLACK IPHONE CELLULAR TELEPHONE, MODEL A1387 (EMC 2430), SEIZED ON OR ABOUT DECEMBER 20, 2014 (the "DEVICE"), further described in Attachment A, the things described in Attachment B, which constitute evidence, fruits and instrumentalities of the knowing and intentional use, attempt to use, or possession of a nonimmigrant visa knowingly procured by means of false statements or fraud, in violation of Title 18, United States Code, Section 1546(a).

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I have been employed as a Special Agent with the DSS since 2013. I have been involved in the investigation of multiple cases involving passport and visa fraud. I am familiar with the facts and circumstances of this investigation set forth below from my own personal participation in the investigation, my review of documents, my training and experience, and from discussions with other law enforcement officers, including, but not limited to, United States Customs and Border Protection ("CBP"), concerning this investigation and other matters involving the use, attempted use, or possession of nonimmigrant visas knowingly procured by false statements or fraud. Statements attributable to individuals herein are set forth in sum and substance and in part, unless otherwise indicated.

BACKGROUND OF THE INVESTIGATION

2. By indictment dated January 5, 2015, JUSTIN EGBUNNE NWANAFORO was charged with knowingly and willfully using and attempting to use a United States visa that was procured by means of a false claim or statement and otherwise procured by fraud and unlawfully obtained, in violation of Title 18, United States Code, Section 1546.

3. On December 20, 2014, the defendant JUSTIN EGBUNNE NWANAFORO arrived at John F. Kennedy International Airport on Arik Airlines flight no. W3 107 from Lagos, Nigeria. The defendant presented a valid Nigerian passport no. A05249437 and a B1/B2 United States entry visa with foil no. J8637903 in the name of JUSTIN EGBUNNE

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

NWANAFORO to a CBP officer. The defendant's B1/B2 visa was issued by the United States Embassy in Abuja, Nigeria on October 17, 2014.

4. The defendant JUSTIN EGBUNNE NWANAFORO was referred for a secondary inspection by CBP officers. During the secondary inspection, the defendant stated, in sum and substance and in part, that he was coming to the United States to inquire about purchasing equipment from a company named U.S. Industrial Machinery Sales Company located in Memphis, TN. The defendant was in possession of an invitation letter from U.S. Industrial Machinery Sales Company. The defendant further claimed to work for a company called Fol Hope Nig. Ltd.

5. Law enforcement officers contacted the owner of U.S. Industrial Machinery Sales Company identified on the letter. The company owner stated, in sum and substance and in part, that the invitation letter was a forgery.

6. The CBP officers notified agents from DSS. DSS agents read the defendant his Miranda rights, which he said he understood and which rights he waived. In the subsequent interview the defendant admitted, in sum and substance and in part, that: (1) he does not work for and never worked for Fol Hope Nig. Ltd.; (2) he paid another individual ("Individual 1") approximately $1800 to assist in completing his visa application; and (3) he was given an invitation letter and a set of common interview questions to study so he could "pass" the interview.

PROBABLE CAUSE TO SEARCH THE DEVICE

7. During the secondary inspection with CBP officers, the defendant JUSTIN EGBUNNE NWANAFORO produced the DEVICE from his person and showed it to CBP officers. The defendant voluntarily provided the DEVICE and the passcode to the DEVICE to CBP officers. On the DEVICE, CBP officers discovered a photograph of the aforementioned invitation letter from U.S. Industrial Machinery Sales Company. CBP officers also discovered photographs of a Nigerian passport and non-immigrant B1/B2 visa for another Nigerian citizen on the DEVICE.

8. During the subsequent interview with DSS agents, the defendant JUSTIN EGBUNNE NWANAFORO unlocked the DEVICE and showed DSS agents the contact information for Individual 1, who prepared and submitted the defendant's visa application. The defendant also showed DSS agents text messages and other communications on the DEVICE between the defendant and Individual 1.

9. The DEVICE has continuously been in the exclusive custody of the CBP since it was seized on or about December 20, 2014. Photographs of the DEVICE are attached as Attachment C.

10. Consistent with the foregoing, and based on my training, experience and discussions with other law enforcement officers, I understand that individuals involved in using, attempting to use, or possessing United States visas knowingly procured by false statements or fraud often do not act alone and regularly communicate by means of cellular telephones such as the DEVICE. Such persons commonly maintain records that reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain

records of communications such as call logs, chats and text messages in their cellular telephones. They commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals usually maintain these records of communication and photographs in their possession and in their cellular telephones.

TECHNICAL TERMS

11. As used herein, the following terms have the following meanings:

a. Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and email; taking, sending, receiving and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device, and a wide variety of applications, also known as "apps," which may store the user's preferences and other data. Such apps may include Facebook, Twitter, and other social media services.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four

numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or other electronic device, such as the DEVICE, that connects to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

12. Based on my research, I understand that the DEVICE provides not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share photographs and videos; and use a wide variety of apps. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICE.

TECHNICAL BACKGROUND

13. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence can be recovered from the DEVICE because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and instant messaging/"chat" programs store

configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, instant messaging or chat logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how

the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

14. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

15. CBP officers seized the DEVICE from the defendant on or about December 20, 2014. Since the seizure, the DEVICE exclusively has been in CBP custody. Because this application seeks only permission to examine the DEVICE, which is already in law enforcement's possession, the execution of the warrant does not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

Based on the foregoing, there is probable cause to believe that the DEVICE contains evidence, fruits, and instrumentalities of instrumentalities of the knowing and intentional use, attempt to use, or possession of a nonimmigrant visa knowingly procured by

means of false statements or fraud, in violation of Title 18, United States Code, Section 1546(a).

Accordingly, the Court should issue the requested warrant.

WHEREFORE, your deponent respectfully requests that a search warrant be issued for the PREMISES KNOWN AND DESCRIBED AS A BLACK IPHONE CELLULAR TELEPHONE, MODEL A1387 (EMC 2430), SEIZED ON OR ABOUT DECEMBER 20, 2014.

Dated: Brooklyn, New York
April 1, 2015

Michael Flaherty
Special Agent
Diplomatic Security Service

Sworn to before me this
1st day of April, 2015

S/ Viktor V. Pohorelsky

THE HONORABLE VIKTOR V. POHORELSKY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK